

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭63-244288

⑬ Int. Cl.<sup>4</sup>

識別記号

庁内整理番号

⑭ 公開 昭和63年(1988)10月11日

G 06 K 17/00  
G 06 F 15/21

340

T-6711-5B  
B-7230-5B

審査請求 未請求 発明の数 1 (全4頁)

⑯ 発明の名称 ICカード暗証照合システム

⑰ 特 願 昭62-77726

⑱ 出 願 昭62(1987)3月31日

⑲ 発 明 者 伊 藤 守 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
 ⑲ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地  
 ⑲ 代 理 人 弁理士 中尾 敏男 外1名

## 明 細 書

## 1. 発明の名称

ICカード暗証照合システム

## 2. 特許請求の範囲

(1) カード所持者が暗証符号を入力する暗証符号入力手段、前記暗証符号入力手段から得られる第1の入力暗証符号を用いて暗号化鍵を生成する暗号化鍵生成手段、および前記暗号化鍵を用いて前記第1の入力暗証符号を暗号化された第2の入力暗証符号に変換する暗証符号暗号化手段を具備する暗証入力装置と、カード発行時などに登録される登録暗証符号を記憶するメモリ手段、および前記登録暗証符号と前記第2の入力暗証符号との照合を行い照合結果を出力する暗証照合手段を具備するICカードと、前記暗証入力装置から得られる第2の入力暗証符号を前記ICカードに書き込み、前記ICカードから前記登録暗証符号と前記第2の入力暗証符号の照合結果を読み出すICカード端末とを有し、前記登録暗証符号を、前記暗号化鍵と同一

の暗号化鍵と前記暗証符号暗号化手段と同一の暗号化鍵を用いて暗号化し、前記メモリ手段に書き込んで記憶させ、暗証照合時には暗号化された暗証符号同士を、復号化することなしに暗証照合を行うことにより、暗証符号を第三者から保護するように構成したICカード暗証照合システム。

(2) 暗号入力装置における暗号化鍵生成手段は、暗号化鍵を生成するのに必要なデータが記憶されているルックアップテーブルメモリからなる特許請求の範囲第1項記載のICカード暗証照合システム。

## 3. 発明の詳細な説明

## 産業上の利用分野

本発明は、主としてキャッシュカード、クレジットカードなどの電子的資金移動(ET)取引に用いられるICカードの正当性を確認するための暗証符号照合システムに関するものである。

## 従来の技術

第3図は、従来のICカード暗証照合システム

における一構成例を示したものである。第3図において、310はICカード所持者が暗証符号を入力する暗証符号入力手段301から得られる入力暗証符号を出力する暗証入力装置、320はカード発行時などに登録される登録暗証符号を記憶するメモリ手段302と、前記登録暗証符号と前記入力暗証符号との照合を行い照合結果を出力する暗証照合手段303から構成されるICカードである。330は前記暗証入力装置310から得られる入力暗証符号を前記ICカード320に書き込み、前記ICカード320から前記登録暗証符号と前記入力暗証符号の照合結果を読み出すICカード端末機である。

以上のように構成された従来のICカード暗証照合システムについて、以下にその動作の説明を行う。

ICカード所持者がICカード320をICカード端末機330に装着した後、暗証符号入力手段301から暗証符号を入力すると、入力された暗証符号は暗証入力装置310から入力暗証符号

暗証符号の利用以外に方法が無く、暗証符号を第三者から保護することはICカードのセキュリティ上、きわめて重要である。

本発明はかかる問題点に鑑みてなされたもので、簡易な構成で暗証符号を第三者から保護することのできるICカード暗証照合システムを提供することを目的としている。

#### 問題点を解決するための手段

本発明は上記問題点を解決するため、カード所持者が暗証符号を入力する暗証符号入力手段、前記暗証符号入力手段から得られる第1の入力暗証符号を用いて暗号化鍵を生成する暗号化鍵生成手段、および前記暗号化鍵を用いて前記第1の入力暗証符号を暗号化された第2の入力暗証符号に変換する暗証符号暗号化手段とを具備する暗証入力装置と、カード発行時などに登録される登録暗証符号を記憶するメモリ手段、および前記登録暗証符号と前記第2の入力暗証符号との照合を行い照合結果を出力する暗証照合手段とを具備するICカードと、前記暗証入力装置から得られる第2の

としてICカード端末機330に入力され、ICカード320内の暗証照合手段303の—入力に加えられる。一方、ICカード320内のメモリ手段302に記憶された登録暗証符号は、前記暗証照合手段303の他の入力に加えられ、入力暗証符号との照合がとられる。ICカード端末機330は暗証符号の照合結果をICカード320から読み取り、カード所持者の本人確認を行う。

#### 発明が解決しようとする問題点

このような従来のICカード暗証照合システムでは、暗号化されていない暗証符号を用いて暗証照合を行うため、暗号化されていない暗証符号が暗証入力装置310からICカード320まで伝送され、カード所有者以外の第三者に暗証符号が伝わる危険性があった。また、このような従来のシステムに用いられるICカード320には、暗号化されていない暗証符号が記憶されるため、カード紛失時にはカード所有者以外に暗証符号が盗まれる可能性があった。現在のICカードを用いた取引において、カード所持者の本人確認には、

入力暗証符号を前記ICカードに書き込み、前記ICカードから前記登録暗証符号と前記第2の入力暗証符号の照合結果を読み出すICカード端末機とを有し、前記登録暗証符号を、前記暗号化鍵と同一の暗号化鍵と前記暗証符号暗号化手段と同一の手続きを用いて暗号化し、前記メモリ手段に覚えもって記憶させ、暗証照合時には暗号化された暗証符号同士を、復号化することなしに暗証照合を行うことにより、暗証符号をカード所有者以外の第三者から保護するように構成したものである。

#### 作用

このように構成されたICカード暗証照合システムにおいて、暗号化鍵生成手段は、暗証符号入力手段から得られる第1の入力暗証符号を用いて暗号化鍵を生成し、暗証符号暗号化手段は、前記暗号化鍵を用いて前記第1の入力暗証符号を暗号化して第2の入力暗証符号に変換し、暗証入力装置は、こうして暗号化された第2の入力暗証符号をICカード端末機に対して出力する。

特開昭63-244288(3)

ICカード端末機は、前記暗証入力装置から得られた第2の入力暗証符号をICカード内に書き込み、ICカードから出力される照合結果を待つ。

一方、メモリ手段は、カード発行時などに登録される登録暗証符号を記憶しておき、暗証照合手段は、前記登録暗証符号と前記第2の入力暗証符号との照合を行い、ICカードは、このようにして照合結果をICカード端末機に提供する。

このとき、前記登録暗証符号を、前記暗号化鍵と同一の暗号化鍵と前記暗証符号暗号化手段と同一の手続きを用いて暗号化し、前記メモリ手段にさえもって記憶させ、暗証照合時には暗号化された暗証符号同士を、復号化することなしに暗証照合することにより、暗証符号をカード所有者以外の第三者から保護することが可能となる。

#### 実施例

以下、本発明の実施例を図面を参照しながら説明する。第1図は、本発明によるICカード暗証照合システムの一実施例を示している。

第1図において、120はメモリ手段104と

暗号化鍵生成手段102と暗証符号暗号化手段103に加えられる。暗号化鍵生成手段102は、暗証符号入力手段101から得られる第1の入力暗証符号PIN1を用いて暗号化鍵KKIを生成し、暗証符号暗号化手段103は、暗号化鍵生成手段102から得られる暗号化鍵KKIを用いて第1の入力暗証符号PIN1を暗号化し、暗証入力装置110はこうして暗号化された第2の入力暗証符号PIN2をICカード端末機130に対して出力する。

ICカード端末機130は、暗証入力装置110から得られる第2の入力暗証符号PIN2をICカード120に書き込み、ICカード120から暗証符号の照合結果ANSが出力されるのを待つ。

一方、ICカード120内のメモリ手段104に記憶されている登録暗証符号PIN3は、暗証照合手段105によって読み出され、ICカード端末機130から入力された第2の入力暗証符号PIN2との暗証照合を行い、ICカード120はこのようにして得られた照合結果ANSをIC

暗証照合手段105から構成されるICカード、130はICカード端末機で、これらは第3図の従来例の構成と同じものである。

101はICカード所持者が暗証符号を入力する手段を提供する暗証符号入力手段、102は暗証符号入力手段101から得られる第1の入力暗証符号PIN1から暗号化鍵KKIを生成する暗号化鍵生成手段、103は暗号化鍵生成手段102から得られる暗号化鍵KKIを用いて第1の入力暗証符号PIN1を暗号化し第2の入力暗証符号PIN2に変換する暗証符号暗号化手段である。

また、110は暗証符号入力手段101と暗号化鍵生成手段102と暗証符号暗号化手段103からなる暗証入力装置である。

以上のように構成されたICカード暗証照合システムについて、以下にその動作の説明を行う。

ICカード所有者がICカード120をICカード端末機130に装着した後、暗証符号入力手段101から暗証符号を入力すると、入力された暗証符号は第1の入力暗証符号PIN1として暗

カード端末機130に対して出力する。

ただし、本実施例における登録暗証符号PIN3は、暗号化鍵生成手段102で生成される暗号化鍵KKIと同一の暗号化鍵と暗証符号暗号化手段103で用いられる暗号化の手段と同一の手続きにより、カード発行時などにさえもって暗号化され、ICカード120内のメモリ手段104に記憶されている。

第2図は、本発明によるICカード暗証照合システムに用いられる暗号化鍵生成手段の一実施例を示している。第2図aは、ルックアップテーブルメモリLUTにより、暗証符号nが暗号化KKInに変換されるようすを模式的に表している。第2図bは、前記ルックアップテーブルメモリLUTに記憶されている変換規則を示している。

第2図において、暗証符号入力手段101から入力される暗証符号nがルックアップテーブルメモリLUTのアドレス入力に加えられると、前記ルックアップテーブルメモリLUTのデータ出力から前記暗証符号nに対応した暗号化鍵KKIn

特開昭63-244288 (4)

が出力される。

#### 発明の効果

以上述べてきたように本発明によれば、簡易な構成で、暗証符号を第三者から保護することができ、ICカードのセキュリティ上、きわめて有用なものとなる。

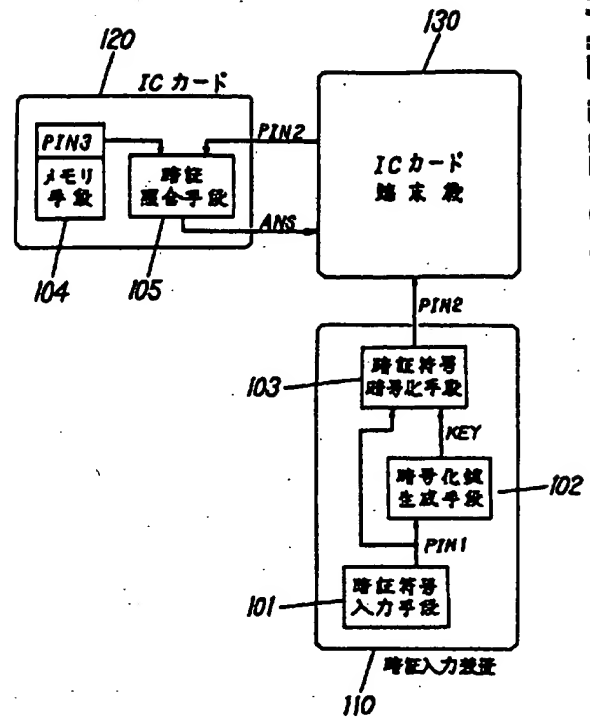
#### 4、図面の簡単な説明

第1図は本発明によるICカード暗証照合システムの一実施例の構成を示す図、第2図は第1図に示した本発明の実施例に用いられた暗号化鍵生成手段の一実施例の構成を示す図、第3図は従来のICカード暗証照合システムの一構成例を示す図である。

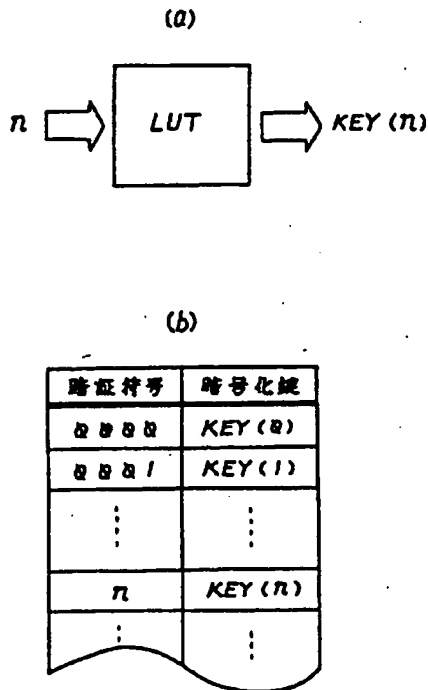
101……暗証符号入力手段、102……暗号化鍵生成手段、103……暗証符号暗号化手段、104……メモリ手段、105……暗証照合手段、110……暗証入力装置、120……ICカード、130……ICカード端末機。

代理人の氏名 弁理士 中 尾 敏 男 ほか1名

第 1 図



第 2 図



第 3 図

